Knowbots, Permissions Headers and Contract Law

.   paper for the conference on

Technological Strategies for Protecting Intellectual
Property in the Networked Multimedia Environment

April 2-3, 1993 with revisions of 4/30/93

Copyright 1993
Henry H. Perritt, Jr.
Professor of Law
Villanova Law School
Villanova, PA 19085
(215) 645-7078
FAX (215) 645-7033, (215) 896-1723
Internet: perritt@ucis.vill.edu

Introduction

One of the ways to protect intellectual property on the
NREN is through a digital library concept. Under this
concept, a work would have attached to it a "permissions
header," defining the terms under which the copyright owner
makes the work available. The digital library
infrastructure, implemented on the NREN, would match request
messages from users with the permissions headers. If the
request message and the permissions header match, the user
would obtain access to the work. This concept encompasses
major aspects of electronic contracting, which is already in
wide use employing Electronic Data Interchange ("EDI")
standards developed by ANSI Committee X12.1

This paper explains the relationship between the digital
library concept and EDI practice, synthesizing appropriate
solutions for contract law, evidence, and agency issues that
arise in electronic contracting. The question of how
electronic signatures should work to be legally effective is
an important part of this inquiry. The paper also defines
particular types of service identifiers, header descriptors,
and other forms of labeling and tagging appropriate to allow
copyright owners to give different levels of permission,
including outright transfer of the copyright interest, use
permission, copying permission, distribution permission,
display permission, and permission to prepare derivative
works.The paper considers how payment authorization
procedures should work in conjunction with a permissions
header and digital library concept in order to integrate the
proposed copyright licensing procedures with existing and
anticipated electronic payment authorization systems. The
paper necessarily considers whether existing standards
approaches related to SGML and X12 are sufficient or whether
some new standards development efforts will be necessary for
implementation of the concepts. The paper considers the
relationship between technology and law in enforcing
intellectual property, and emphasizes that the traditional
adaptation of legal requirements to levels of risk is
appropriate as the law is applied to new technologies.

There are certain common issues between the intellectual property question and other applications of wide area digital network technology. The question of signatures and writings to reflect the establishment of duties and permissions and the transfer of rights is common to the intellectual property inquiry and to electronic commerce using EDI techniques. There also are common questions involving rights to use certain information channels: First Amendment privileges, and tort liability. These are common not only to technological means of protecting intellectual property but to all forms of wide area networking.

The problem

The law recognizes intellectual property because information technology permits one person to get a free ride on another person's investment in creating information value. Creative activity involving information usually is addressed by copyright, although patent has a role to play in protecting innovative means of processing information.2

Intellectual property arose in the context of letterpress printing technology. Newer technologies like xerography and more recently small computer technology and associated word processing and networking have increased the potential for free rides and accordingly increased the pressure on intellectual property.

The concern about free ride potential is especially great when people envision putting creative works on electronic publishing servers connected to wide area networks intending to permit consumers of information products to access these objects, frequently combining them and generally facilitating "publishing on demand" rather than the well known publishing just in case, typified by guessing how many copies of a work will sell, printing those in advance, and then putting them in inventory until someone wants them.

The concern is that it will be too easy to copy an entire work without detection and without paying for it. Worse, it will be easy to copy an entire work and resell it either by itself or as a part of a new derivative work or collection.

But technology is capable of protecting investment in new ways as well as gaining a free ride. Computer networks make it possible to restrict access and to determine when access occurs. Depending on how new networks are designed, they may actually reduce the potential for a free ride. The digital library is one way of realizing that potential. Professor Pamela Samuelson has observed that the digital library model replaces intellectual property with a system of technological controls.3

Digital Library Concepts
  Basic Concepts

A digital library is a set of information resources ("information objects") distributed throughout an electronic network. The objects reside on servers (computers with associated disk drives connected to the network). They can be retrieved remotely by users using "client" workstations.
  Origin of Concepts

The phrase "digital library" and the basic concept was first articulated in a 1989 report growing out of a workshop sponsored by the Corporation for National Research Initiatives.4 From its inception, the digital library concept envisioned retrieval of complete information resources and not merely bibliographic information.5

The technologies of remote retrieval of complete information objects using electronic technologies is in wide use through the WESTLAW, Dialog, LEXIS, NEXIS, and National Library of Medicine databases. These remotely accessible databases, however, unlike the digital library involved a single host on which most of the data resides. The digital library concept envisions a multiplicity of hosts (servers).
    Recent Developments

The remotely accessible database host concept is converging with the digital library concept as more of the electronic database vendors provide gateways to information objects actually residing on other computers. This now is commonplace with WESTLAW access to Dialog, and Dialog's gateways to other information providers.

The most explicit implementation of the digital library concept is the Wide Area Information Service ("WAIS"), which implements ANSI standard Z.39.6 WAIS permits a remote user to formulate a query that is applied to a multiplicity of WAIS servers each of which may contain information responsive to the query. The WAIS architecture permits search engines of varying degrees of sophistication, resident on WAIS information servers to apply the query against their own information objects, reporting matches back to the user.7 Future implementations of WAIS permit automatic refinement of searches according to statistical matching techniques.

The Corporation for National Research Initiatives has proposed a test bed for an electronic copyright management system.8 The proposed system would include four major elements: automated copyright recording and registration, automated, on line clearance of rights, private electronic mail and digital signatures to provide security. It would include three subsystems: a Registration and Recording System (RRS), a Digital Library System (DLS), and a Rights Management System (RMS). The RRS would provide the functions enumerated above and would be operated by the Library of Congress. It would provide "change of title" information.9 The RMS would be an interactive distributed system capable of granting rights on line and permitting the use of copyrighted material in the Digital Library System. The test bed architecture would involve computers connected to the Internet performing the RRS and RMS functions.

Digital signatures would link an electronic bibliographic record with the contents of the work, ensuring against alteration after deposit.10 Multiple RMS servers would be attached to the Internet. A user wishing to obtain rights to an electronically published work would interact electronically with the appropriate RMS. When copyright ownership is transferred, a message could be sent from the RMS to the RRS11 - creating an electronic marketplace for copyrighted material.

The EBR submitted with a new work would "identify the

rights holder and any terms and conditions on the use of the document or a pointer to a designated contact for rights and permissions."12 The EBR, thus, is apparently equivalent to the permissions header discussed in this paper. Security in the transfer of rights would be provided by digital signatures using public key encryption, discussed further, infra in the section on encryption.

Basic Architectural Concepts

The digital library concept in general contemplates three basic architectural elements: a query, also called a "knowbot" in some descriptions; a permissions header attached to each information object; and a procedure for matching the query with the permissions header.

Two kinds of information are involved in all three architectural elements: information about the content of information objects desired and existing, and information about the economic terms on which an information object is made available. For example, a query desiring court opinions involving the enforcement of foreign judgments evidencing a desire to download the full text of such judicial opinions and to pay up to $1.00 per minute of search and downloading time would require that the knowbot appropriately represent the subject matter "enforcement of foreign judgments." It also requires that the knowbot appropriately represent the terms on which the user is willing to deal: downloading and the maximum price. The permissions header similarly must express the same two kinds of information. If the information object to which the permissions header is attached is a short story rather than a judicial opinion, the permissions header must so indicate. Or, if the information object is a judicial opinion and it is about enforcement of foreign judgments, the permission header may indicate that only a summary is available for downloading at a price of $10.00 per minute. The searching, matching, and retrieval procedure in the digital library system must be capable of determining whether there is a match on both subject matter and economic terms, also copying and transmitting the information object if there is a match.

Comparison to EDI

Electronic Data Interchange ("EDI") is a practice involving computer-to-computer commercial dealing without human intervention. In the most widespread implementations, computers are programmed to issue purchase orders to trading partners, and the receiving computer is programmed to evaluate the terms of the purchase order and to take appropriate action, either accepting it and causing goods to be manufactured or shipped or rejecting it and sending an appropriate message. EDI is in wide use in American and foreign commerce, using industry-specific standards for discrete commercial documents like purchase orders, invoices, and payment orders, developed through the American National Standards Institute.

There obviously are similarities between the three architectural elements of the digital library concept and EDI. There is a structured way of expressing an offer or instruction, and a process for determining whether there is a match between what the recipient is willing to do and what the sender requests.

There is also, however, an important difference. In the digital library concept, a match results in actual delivery

of the desired goods and services in electronic form. In EDI
practice, the performance of the contractual arrangement
usually involves physical goods or performance of
nonelectronic services.

Nevertheless, the digital library and EDI architectures
are sufficiently similar and, it turns out the legal issues
associated with both are sufficiently similar to make
analogies appropriate.

Elements of Data Structure

For purposes of this paper, the interesting parts of the
data structure are those elements that pertain to
permission, more than those elements that pertain to content
of the information object to which the header is attached.
Accordingly, this section will focus on only permissions-
related elements, after noting in passing that the content
part of the header well might be a pointer to an inverted
file to permit full text searching and matching.

The starting point conceptually for identifying the
elements of the permissions header are the rights
exclusively reserved to the copyright owner by 106 of the
copyright statute. But these exclusive rights need not be
tracked directly because the owner of an information object
free to impose contractual restrictions as well as to enjoy
rights granted by the Copyright Act. Accordingly, it seems
that the following kinds of privileges in the requester
should be addressed in the permissions header:

   outright transfer of all rights

   use privilege, either unrestricted or subject to
    restrictions

   copying, either unlimited or subject to restrictions
    like quantitative limits

   distribution, either unlimited or subject to
    restrictions, like geographic ones or limits on the
    markets to which distribution can occur

   preparation of derivative works

   Display and presentation rights, separately identified
in 106 would be subsumed into the use element, because
they are particular uses.

The simplest implementation would allow only binary
values for each of these elements. But a binary approach
does not permit the permissions header to express
restrictions, like those suggested in the enumerated list.
Elements could be defined to accept the most common kinds of
restrictions on use, and quantitative limits on copying, but
it would be much more difficult to define in advance the
kinds of geographic or market-definition restrictions that
an owner might wish to impose with respect to distribution.

In addition to these discrete privileges, the
permissions header must express pricing information. The
most sensible way of doing this is to have a price
associated with each type of privilege. In the event that
different levels of use, copying, or distribution privilege
are identified, the data structure should allow a price to

be associated with each level.

A complicating factor in defining elements for price is the likelihood that different suppliers would want to price differently. For example, some would prefer to impose a flat fee for the grant of a particular privilege. Others might wish to impose a volume-based fee, and still others might wish to impose a usage or connect-time based fee. The data structure for pricing terms must be flexible enough to accommodate at least these three different approaches to pricing.

Finally, the data structure must allow for a specification of acceptable payment terms and have some kind of trigger for a payment approval procedure. For example, the permissions header might require presentation of a credit card number and then trigger a process that would communicate with the appropriate credit card database to obtain authorization. Only if the authorization was obtained would the knowbot and the permissions header "match."

There is a relationship between the data structures and legal concepts. The knowbot is a solicitation of offers. The permissions header is an offer. The matching of the two constitutes an acceptance. Mr. Linn's "envelope" could be the "contract."

There are certain aspects of the data structure design that are not obvious. One is how to link price with specific levels of permission. Another is how to describe particular levels of permission. This representation problem may benefit from the use of some deontic logic, possibly in the form of a grammar developed for intellectual property permissions. Finally, it is not clear what the acceptance should look like. Conceptually, the acceptance occurs when the knowbot matches with a permissions header, but it is unclear how this legally significant event should be represented.

Role of Encryption

The CNRI test bed proposal envisions the use of public key encryption to ensure the integrity of digital signatures and to ensure the authenticity of information objects. Public key encryption permits a person to encrypt a message - like a signature using a secret key, one known only to the sender, while permitting anyone with access to a public key to decrypt it. Use of public key cryptography in this fashion permits any user to authenticate a message, ensuring that it came from the purported sender.13 A related technology called "hashing" permits an encrypted digital signature to be linked to the content of a message. The message can be sent in plain text (unencrypted) form, but if any part of it is changed, it will not match the digital signature. The digital signature and hashing technologies thus permit not only the origin but also the content integrity of a message of arbitrary length to be authenticated without necessitating encryption of the content of the message. This technology has the advantage, among others, that it is usable by someone lacking technological access to public key encryption. An unsophisticated user not wishing to incur the costs of signature verification nevertheless can use the content of the signed information object.

It is well recognized that encryption provides higher levels of security than other approaches. But security through encryption comes at a price. Private key encryption systems require preestablished relationships and exchange of private keys in advance of any encrypted communication. The burdens of this approach have led most proponents of electronic commerce to explore public key encryption instead. But public key systems require the establishment and policing of a new set of institutions. An important infrastructure requirement for practicable public key cryptography is the establishment and maintenance of certifying entities that maintain the public keys and ensure that they are genuine ones rather than bogus ones inserted by forgers. A rough analogy can be drawn between the public key certifying entities and notaries public. Both kinds of institutions verify the authenticity of signature. Both kinds require some level of licensing by governmental entities. Otherwise the word of the "electronic notary" (certifying entity) is no better than an uncertified, unencrypted signature. In a political and legal environment in which the limitations of regulatory programs have been recognized and have led to deregulation of major industries, it is not clear that a major new regulatory arrangement for public key encryption is practicable. Nevertheless, experimentation with the concept in support of digital library demonstration programs can help generate more empirical data as to the cost and benefits of public key encryption to reinforce electronic signatures.

On the other hand, it is not desirable to pursue approaches requiring encryption of content. No need to encrypt the contents is apparent in a network environment. Database access controls are sufficient to prevent access to the content if the permissions header terms are not matched by the knowbot. On the other hand, if the electronic publishing is effected through CDROMs or other physical media possessed by a user, then encryption might be appropriate to prevent the user from avoiding the permissions header and going directly to the content.

While encrypted content affords greater security to the owner of copyrighted material. Someone who has not paid the price to the copyright owner must incur much higher cost to steal the material. But the problem is everyone must pay a higher price to use the material. One of the dramatic lessons of the desktop computer revolution was the clear rejection of copyright protection in personal computer software. The reasons that copy protection did not survive in the market place militate against embracing encryption for content. Encryption interferes with realization of electronic markets, because producer and consumer must have the same encryption and description protocols. Encryption burdens processing of electronic information objects because it adds another layer. Some specific implementations have encryption require additional hardware at appreciable costs.

Digital libraries cannot become a reality until consumers perceive that the benefits of electronic formats outweigh the costs, compared to paper formats. Encryption interferes with electronic formats' traditional advantages of density, reusability, editability, and computer search ability and also, by impairing open architectures may perpetuate some of papers' advantages with respect with browsibility.14

The need for encryption of any kind depends upon whether
security is available without it. That depends, in turn, on
the kinds of free rides that may be obtainable and the legal
status of various kinds of electronics transactions in the
digital library system.

Legal Issues
    Copyright: What legal effect is intended?

The design of the permissions header and the values in
the elements of the header must be unambiguous as to whether
an outright transfer of a copyright interest is intended or
whether only a license is intended. If an outright transfer15
is intended, then the present copyright statute requires a
writing signed by the owner of the rights conveyed.16
Recordation of the transfer with the Copyright office is not
required, but provides advantages in enforcing transferee
rights.17 On the other hand, non exclusive licenses need not
be in writing nor registered. If the electronic transaction
transfers the copyright in its entirety, then the rights of
the transferor are extinguished, and the rights of the
transferee are determined by the copyright statute. The only
significant legal question is whether the conveyance was
effective.

On the other hand, when the copyright is not transferred
outright but only certain permissions are granted or certain
rights conveyed, the legal questions become more varied.
Then, the rights of the transferor and the obligations of
the transferee are matters of contract law. It is important
to understand the degree to which the contract is
enforceable and how it is to be interpreted in the event of
subsequent disputes. The following sections consider briefly
the first sale doctrine as a potential public policy
obstacle to enforcing contractual restrictions different
from those imposed by the copyright statute and then explore
in greater depth whether electronic techniques satisfy the
formalities traditionally required for making a contract,
whether they adequately ensure against repudiation, and
whether they provide sufficient information to permit
predictable interpretation of contractual obligations and
privileges.
    First Sale Doctrine

The first sale doctrine may invalidate restrictions on
use. It is impermissible for the holder of a patent to
impose restrictions on the use of a patented product after
the product has been sold. Restrictions may be imposed,
however, on persons who merely license the product.18 The
rationale for this limit on the power of the owner of the
intellectual property interest is that to allow limitations
on use of the product would interfere with competition
beyond what the Congress - and arguably the drafters of the
Constitution - intended in setting up the patent system.

The first sale doctrine applies to copyright owners.19
Indeed, because of the First Amendment's protection of
informational activity, the argument against restrictions
after the first sale may be even stronger in the copyright
arena then in the patent arena.

The first sale doctrine is potentially important because
it may invalidate restrictions imposed on the use of
information beyond what is authorized by the Copyright Act
and by common law trade secret. Thus, there may be serious

questions about the legal efficacy of use restrictions
suggested in ___, although such restrictions are common in
remote database service agreements. The vendors could argue
that the limitations pertain to the contractual terms for
delivery of a service rather than use of information as
such. The characterization avoids the overlap with copyright
and thus may also avoid the conflict between federal policy
and contract enforcement.20

Contract Formation Issues

The law does not enforce every promise. Instead, it
focuses its power only on promises surrounded with certain
formalities to make it likely that the person making the
promise (the "promisor") and the person receiving the
promise (the "promisee") understood that their communication
had legal consequences. A threshold question for the digital
library system is whether the traditional formalities for
making a contract are present when the contract is made
through electronic means. The digital library system
considered in this paper clearly contemplates that a
contract is formed when the knowbot and the permissions
header achieve a match. In this respect, the digital library
concept converges with EDI where trading parties contemplate
that a contract to perform services or deliver goods is
formed when a match occurs either upon the receipt of a
purchase order or upon the transmission of a purchase order
acknowledgment.

It is not altogether clear, however, whether the match
between values and computer data structures meets contract
formation requirements, particularly those expressed in
various statutes of frauds. Statutes of frauds require
"writings" and "signatures" for certain kinds of contracts -
basically those contemplating performance extending beyond a
period of one year.21

In many instances, the digital library contract will be
fully performed almost instantaneously upon delivery of the
information object after the knowbot and the permissions
header match. In such a case, the statute of frauds is not a
problem and its requirements need not be satisfied. In other
cases, however, as when the intent of the owner of the
information object is to grant a license to do things that
will extend beyond one year, the statute of frauds writing
and signature requirements must be met.

Historical application of Statutes Of Frauds by the
courts clearly indicates that there is flexibility in the
meaning of "writing" and "signature." A signature is any
mark made with the intent that it be a signature.22 Thus an
illiterate person signs by making an "X," and the signature
is legally effective. Another person may sign a document by
using a signature stamp. Someone else may authorize an agent
to sign his name or to use the signature stamp. In all three
cases the signature is legally effective. There may of
course be arguments about who made the X, or whether the
person applying the signature stamp was the signer or his
authorized agent, but these are evidentiary and agency
questions, not arguments about hard and fast contract-law
requirements.

Under the generally accepted legal definition of a
signature, there is no legal reason why the "mark" may not
be made by a computer printer, or for that matter by the
write head on a computer disk drive or the data bus in a

computer random access memory. The authorization to the computer agent to make the mark may be given by entering a PIN ("Personal Identification Number") on a keyboard. To extend the logic, there is no conceptual reason to doubt the legal efficacy of authority to make a mark if the signer writes a computer program authorizing the application of a PIN upon the existence of certain conditions that can be tested by the program. The resulting authority is analogous to a signature pen that can be operated only with a mechanical key attached to somebody's key ring, coupled with instructions to the possessor of the key.

Which of these various methods should be selected for particular types of transactions must depend, not on what the law requires, because the law permits any of these methods. Rather, it must depend on the underlying purposes of the legal requirement and which method best serves those purposes.

The real issue is how to prove that a particular party made the mark. In other words, the contingency to be concerned about is repudiation, not absence of formalities. Repudiation should be dealt with through usual evidentiary and fact finding processes rather than artificial distinctions between signed and unsigned documents.

Authority is skimpier on how flexible the "writing" requirement is. The best approach is to borrow the fixation idea from the copyright statute and conclude that a writing is "embodiment in a copy . . . sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for more a period of more than transitory duration."23

The most important thing conceptually is to understand the purpose of the writing and signature requirements. They have two purposes: awareness or formality and reliability of evidence. Signature requirements, like requirements for writings and for original documents have an essentially evidentiary purpose. If there is a dispute later, they specify what kind of evidence is probative of certain disputed issues, like "who made this statement and for what purpose?" The legal requirements set a threshold of probativeness. Surely the values in a knowbot as well as the values in a permissions header constitute and "mark," and someone who knowingly sets up potential transactions in a digital library scheme can have the intent that the mark be a signature.

When a contract is made through a signed writing, it is more likely that the parties to the contract understand what they are doing. They are aware of the legal affect of their conduct because the writing in the signature involve a greater degree of formality than a simple conversation.

The awareness/formality purpose can be served by computerized contracting systems. This is so not so much because the computers are "aware" of the affect of their "conduct." Rather, it is true because the computers are agents of human principals. The programming of the computer to accept certain contract terms is the granting of authority to the computer agent to enter into a contract. The fact that a principal acts through an agent engaging in conduct at a later point and time never has been thought to defeat contract formation in the traditional evolution of

agency and contract law. Nor should it when the agent is a computer.

Fulfillment of the evidentiary purpose depends on the reliability of the information retained by the computer systems making up the digital library. Such systems must be designed to permit the proponent of contract formation to establish the following propositions if the other party to the purported contract attempts to repudiate it.

1. It came from computer X

2. It accurately represents what is in computer X[24] now[25]

   3. What is in computer X now is what was in computer X at the time of the transaction

4. What was in computer X at the time of the transaction is what was received from the telecommunications channel[26]

5. What was received from the telecommunications channel is what was (a) sent, (b) by computer Y.

Two other questions relate to matters other than the authenticity of the message:

6 Computer Y was the agent of B

7 The message content expresses the content of the contract (or more narrowly, the offer or the acceptance).[27]

Factual propositions 1-4 can be established by testimony as to how information is written to and from telecommunications channel processors, primary storage, and secondary storage. Factual proposition 5 requires testimony as to the accuracy of the telecommunications channel and characteristics of the message that associate it with computer Y. Only the last proposition (number 5) relates to signatures, because signature requirements associate the message with its source.[28] The other propositions necessitate testimony as to how the basic message and database management system works. It is instructive to compare these propositions with the kinds of propositions that must be established under the business records exception to the hearsay rule when it is applied to computer information.

Those propositions may be supported with non technical evidence, presented by non programmers. A witness can lay a foundation for admission of computer records simply by testifying that the records are generated automatically and routinely in the ordinary course of business. The more inflexible the routine, and the less human intervention in the details of the computer's management of the database the better the evidence.[29]

The ultimate question is trustworthiness, and if the computer methods are apparently reliable, the information should be admitted unless the opponent of admissibility can raise some reasonable factual question undercutting trustworthiness.[30]

Contract Interpretation Issues

Assuming that the permissions header and knowbot

constitute sufficient writings to permit a contract to be formed and that the signature requirement also is met, through digital signature technology or otherwise, there still are difficult contract interpretation questions. Contract interpretation questions arise not only after contractual relationships are formed, but also in connection with deciding whether there has been offer and acceptance, the prerequisites to contract formation.31 Contract interpretation always seeks to draw inferences about what the parties intended. When contract interpretation issues arise at the contract formation stage, the questions are what the offeror intended the content of the offer to be and what the offeree intended the content of the purported acceptance to be. The proposed Digital Library System envisions extremely cryptic expressions of offer and acceptance - by means of codes. The codes have no intrinsic meaning. Rather, extrinsic reference must be made to some kind of table, standard, or convention associating particular codes with the concepts they represent. Extrinsic evidence is available to resolve contract interpretation questions when the language of the contract itself is ambiguous, and perhaps at other times as well.32 The codes in the permissions header and knowbots certainly are ambiguous and become unambiguous only when extrinsic evidence is considered. So there is no problem in getting a standard or cable into evidence. The problem is whether the parties meant to assent to this standard.

In current EDI practice, this question is resolved by having parties who expect to have EDI transactions with each other to sign a paper trading partner agreement, in which the meaning of values or codes in the transaction sets is established.33 But requiring each pair of suppliers and users of information in a digital library to have written contracts with each other in advance would defeat much of the utility of the digital library. Thus the challenge is to establish some ground rules for the meaning of permissions header and knowbot values that all participants are bound by. There are analogous situations. One is a standard credit card agreement that establishes contractual terms among credit card issuer, credit card subscriber, and merchant who accepts the credit card. The intermediary - the credit card company - unilaterally establishes contract terms to which the trading partners assent by using and accepting the credit card.34 Also, it is widely recognized that members of a private association can, through their constitution and bylaws establish contractual relationships that bind all of the members in dealing with each other.35 In the Digital Library System, similar legal arrangements can establish the standards by which electronic transactions between permissions header and knowbots will bind transferor and transferee of information.
Third Party Liability

It is not enough merely to ensure that the licensee is contractually bound. Trading partners also must ensure that the participants in funds transfers have enforceable obligations. For example, if the digital library system envisions that the information object would not be released to the purchaser without simultaneous release of a payment order, the supplier may be interested in enforcing the obligations of financial intermediaries who handle the payment order. This implicates the federal Electronic Funds Transfer Act, and Article 4A of the Uniform Commercial Code, regulating wire transfers.

Solutions
     Satisfy the Business Records Exception to the Hearsay
Rule

     The discussion of contract formalities earlier in this
paper concluded that legally enforceable contracts can be
formed through electronic means and that the significant
legal questions relate to reliability of proof and intent of
the parties to be bound by using the electronic techniques.
This section considers the reliability of proof further.
Traditional evidence law permits computer records to be
introduced in evidence when they satisfy the requirements of
the business records exception: basically that they are made
in the ordinary course of business, that they are relied on
for the performance of regular business activities, and that
there is no independent reason for questioning their
reliability.36

The business records exception shares with the
authentication concept statute of frauds and the parol
evidence rule a common concern with reliability.37 The same
procedural guarantees and established practices that ensure
reliability for hearsay purposes also ensure reliability for
the other purposes. Under the business records exception,
the proponent must identify the source of a record, through
testimony by one familiar with a signature on the record, or
circumstantially.38 The steps in qualifying a business record
under the common law, which since have been relaxed,39 were:

  Proving that the record is an original entry made in the
  routine course of business

  Proving that the entries were made upon the personal
  knowledge of the proponent/witness or someone reporting
  to him

  Proving that the entries were made at or near the time of
  the transaction

  Proving that the recorder and his informant are
  unavailable.40

     These specific requirements are easier to understand and
to adapt to electronic permissions and obligations formed in
a digital library system by understanding the rationale for
the business records exception. The hearsay rule excludes
out of court statements because they are inherently
unreliable, primarily because the maker of the statement's
demeanor cannot be observed by the jury and because the
maker of the statement is not subject to cross examine. On
the other hand, there are some out of court statements that
have other guarantees of reliability. Business records are
one example. If a continuing enterprise finds the records
sufficiently reliable to use them in the ordinary course of
business, they should be reliable enough for a court. The
criteria for the business records exception all aim at
ensuring that the records really are relied upon the
business to conduct its ordinary affairs.

     The Manual for Multidistrict Litigation suggests steps
for qualifying computer information under the business
records exception:

     1.The document is a business record

2.The document has probative value

3.The computer equipment used is reliable

4.Reliable data processing techniques were used[41]

The key in adapting the business records exception to electronic permissions in a digital library system are points 3 and 4. Establishing these propositions and the propositions set forth in section ___ of this paper requires expert testimony. Any designer of a digital library system must consult with counsel and understand what testimony an expert would give to establish these propositions. Going through that exercise will influence system design.
    Reinforce the Evidentiary Reliability by Using Trusted Third Parties

The evidentiary purpose of contract formation requirements can be satisfied by using a trusted third party as an intermediary, when the third party maintains archival records of the transactions. The third party lacks any incentive for tampering with the records and when the third parties archiving system is properly designed, it can provide evidence sufficient to establish all of the propositions identified in ___ .

This third party intermediary concept is somewhat different from the concept for a certifying agent in digital signature systems. To be sure, the custodian of transaction records envisioned by this section could be the same as the certifying entity for public and key encryption, but the custodian role can be played in the absence of any encryption. Indeed, the digital library itself is a good candidate for the custodian role. The library has no incentive to manipulate its records in favor of either of the producers of information value or the consumers. In order to carry out its affairs, it must use these transactional records in the ordinary course of business, thereby making it likely that digital library records would qualify under the business records exception.
    Standardization

Obviously, the digital library concept depends upon the possibility of an automated comparison between the knowbot and the permissions header. This means that potential requesters of information and suppliers of information must know in advance the data structures for representing the elements of the permissions header and the knowbot. This requires compatibility. Compatibility requires standardization. Standardization does not, however, necessarily require "Standard" in the sense that they are developed by some bureaucratic body like ANSI. It may simply imply market acceptance of a particular vendor's approach. Indeed, each digital library might use different data structures. All that is necessary is that the structure of the knowbot and the structure of the permissions header be compatible within any one digital library system. Also, as demands emerge for separate digital libraries to communicate with each other, there can be proprietary translation to assure compatibility between systems much as common word processing programs translate to and from other common formats and much as printers and word processing software communicate with each other through appropriate printer drivers. In neither of these cases has any independent

standards organization developed a standard that is at all
relevant in the marketplace.

Standardizing the elements of Knowbot and permissions
headers involves content standardization, which generally is
more challenging than format standardization.42 A permissions
header/Knowbot standard is a system for representing legal
concepts and for defining legal relations. As such, the
standard is basically a grammar for a rule based substantive
system in a very narrow domain.43 The data elements must
correspond to legally meaningful relational attributes. The
allowable values must correspond to legally allowable
rights, obligations, privileges and powers. In other words,
the standard setter must meet many of the challenges that a
legal expert system designer working with Hohfeldian
frameworks must meet.44 This adds a constraint to the
standards setting process. Unlike setting format standards,
where the participants are free to agree on an arbitrary way
of expressing format attributes, participants in setting a
content standard must remain within the universe of
permissible content. The set of permissible values is
determined by the law rather than being determined only by
the imagination of format creators.

Enforcement and Bottlenecks

One of the many profound observations by Ithiel de Sola
Pool was that copyright always has depended upon
technological bottlenecks for its enforceability. The
printing press was the original enforcement bottleneck.
Now, a combination of the printing press and the practical
need to inventory physical artifacts representing the work
constitute the enforcement bottlenecks. As technologies
change, old bottlenecks disappear and enforceability
requires a search for new bottlenecks. When there are single
hosts, like Westlaw, Dialog, Lexis, and CompuServe, access
to that host is the bottleneck. The problem with distributed
publishing on an open architecture internet is that there is
no bottleneck in the middle of the distribution chain
corresponding to the printer, the warehouse or the single
host.

If new bottlenecks are to be found, they almost surely
will be found at the origin and at the point of consumption.
Encryption and decryption techniques discussed elsewhere in
this volume concentrate on those bottlenecks as points of
control. It also is possible that rendering software could
become the new bottleneck as Mr. Linn suggests.

Even with those approaches, however, a serious problem
remains in that the new technologies make it difficult or
impossible to distinguish between mere use and copying.
Thus the seller cannot distinguish between an end user45 and
a potential competitor. On the other hand, the new
technologies permit a much better audit trail, potentially
producing better evidence for enforcement adjudication.

If network architectures for electronic publishing
evolve in the way that Ted Nelson suggests with his Xanadu
concept, the real value will be in the network and the
pointers, not in the raw content. Thus, the creative and
productive effort that the law should reward is the creation
and productive effort that the law should reward is the
creation and production and delivery of pointers,
presentation, distribution, and duplication value. If this

is so, then technological means will be particularly important, foreclosing access by those lacking passwords and other keys and limiting through contract what a consumer may do with the information.

In such an architecture, the law either will be relatively unimportant because technology can be counted on to prevent free riding or, the law will need to focus not on prohibiting copying or use without permission, but on preventing circumvention of the technological protections. Thus, legal approaches like that used to prevent the sale of decryption devices for television broadcasts and legal issues associated with contract enforcement may be more important than traditional intellectual property categories.

Weighing Risks and Costs

The law generally imposes sensible levels of transaction costs. Usually, transaction costs are proportional to the risk. Figure 1 shows a continuum of risk and transaction cost in traditional and new technologies. A real estate closing involves significant risks if there is some dispute later about the transaction. Therefore, the law affords much protection, including a constitutional officer called a registrar of deeds who is the custodian of records associated with the transaction. The risk level analogous to this in electronic publishing might be access to an entire library including access software as well as contents. Next, is a transaction involving a will or power of attorney. There, the risk is substantial because the maker of the instrument is not around to help interpret it. The law requires relatively high levels of assurance here, though not as great as those for real estate transactions. The law requires witnesses and attestation by a commissioned minor official called a notary public. The electronic publishing analogy of this level of risk might be the contents of an entire CDROM.

Next, in level of risk is the purchase of a large consumer durable like an automobile. The law requires somewhat less, but still significant protections for this kind of transaction: providing for the filing and enforcement of financing statements under the Uniform Commercial Code. The electronic publishing analogy might be the transfer of copyright to a complete work. Next, down the risk continuum, is the purchase of a smaller consumer durable like a television set. Here, the law typically is reflected in written agreements of sale, but no special third party custodial mechanisms. The electronic publishing analogy might be use permission for a complete work.

Finally, is the purchase of a relatively small consumer item, say a box of diskettes. Neither the law or commercial practice involves much more than the exchange of the product for payment, with no written agreement or anything else to perform channeling, cautionary, evidentiary, or protective functions [make sure these function and the citation appears earlier]. The electronic publishing analogy might be use permission for part of a work.

Cost effectiveness = risk-proportional security

traditional transaction   institutions   electronic
equivalent

real estate closing library - software and	registrar of deeds	entire contents
will/power of attorney entire CDROM	witnesses, notary public	contents of
auto purchase work - transfer of	UCC financing statement	complete copyright
television set purchase work - use permission	written sale agreement	complete
box of diskettes work - use	-	part of a permission

An encrypted object combined with rendering software is probably inconsistent with an open architecture. Because of the difficulty of setting standards for such technologies, this approach to intellectual property protection probably would be effectuated by proprietary approaches thus frustrating the vision of an open market for electronic publishing.

Conclusion

Realization of the digital library vision requires a method for collecting money and granting permission to use works protected by intellectual property. The concept of a knowbot and a permissions header attached to the work is the right way to think about such a billing and collection system. Standards for the data structures involved must be agreed to, and systems must be designed to satisfy legal formalities aimed at ensuring awareness of the legal significance of transactions and reliable proof of the terms of the transactions.

In the long run, not only must these technological issues be resolved, with appropriate attention to levels of risk and protections available under traditional legal doctrines, but also further conceptual development must be undertaken. Proponents of electronic publishing over wide area networks need to think about the appropriate metaphors: whether it is a library or a bookstore, if a library whether with or without xerox machines, if a bookstore whether it is a retail bookstore, or a mail order operation. Then, thought must be given to how standards will be set. Finally, and most important, much more needs to be understood about the need for third party institutions. There is a good deal of enthusiasm for public key encryption. Yet the vulnerability of public key encryption systems is in the integrity of the key authority. In traditional legal protections, the third party custodians or authenticating agents like notary public and registrars of deeds receive state sanction and approval, and in the case of registrars of deeds, public funding. We must be clearer as to whether a similar infrastructure must be developed to protect against substantial risks and the use of EDI and electronic publishing technologies.

Finally, and perhaps most importantly, we must be thoughtful about what legal obligations, imposed on whom,

are appropriate? The suggested 102(e) and (f) in the High
Performance Computing Act looks very much like King James
I's licensing of printing presses. It also looks like the
FBI's proposal to prohibit the introduction of new
technologies until certain conformity with past legal
concepts is assured. Such approaches make the law a hurdle
to new technology -- an uncomfortable position for both law
and technology.

---

1 The use of EDI techniques to meter usage and determine
charges for use of intellectual property is an example of
billing and collection value in a typology of different
types of value that can be produced in electronic
marketplaces for information. See Henry H. Perritt, Jr.,
Market Structures for Electronic Publishing and Electronic
Contracting in Brian Kahin, ed., Building Information
Infrastructure: Issues in the Development of the National
Research and Education Network (Harvard University and
McGraw-Hill 1992) (developing typology for different types
of value and explaining how market structures differ for the
different types); Henry H. Perritt, Jr., Tort Liability, the
First Amendment, and Equal Access to Electronic Networks, 5
Harv.J.Law & Tech. 65 (1992) (using typology of ten types of
value to analyze access by competing producers of value).

2 See, e.g.U.S.Pat. No. 5,016,009, Data compression
apparatus and method (May 14, 1991); U.S. Pat. No.
4,996,690, Write operator with gating capability (Feb. 26,
1991);U.S. Pat. No. 4,701,745, Data compression system (Oct.
20, 1987); Multi Tech Systems, Inc. v. Hayes Microcomputer
Products, Inc., 800 F. Supp. 825 (D. Minn. 1992) (denying
summary judgment on claim that patent for modem escape
sequence is invalid)..

3 Comments on the 8\21 draft of "Knowbots in the Real
World" from the intellectual property workshop participants
at page 6 (author unknown, source unknown). Professor
Samuelson also observed that the workshop, despite its
title, actually did not focus much on intellectual property
issues.

4 Corporation for National Research Initiatives,
Workshop On The Protection Of Intellectual Property Rights
In A Digital Library System: Knowbots in the Real World-May
18-19, 1989 (describing digital library system).

5 See generally Clifford A. Lynch, Visions of Electronic
Libraries (libraries of future can follow acquisition-on-
demand model rather than acquiring an advance of use; Z39.50
protocol will facilitate realization of that possibility,
citing Robert E. Kahn & Vinton G. Serf, An Open Architecture
for a Digital Library System and a Plan for Its Development.
The Digital Library Project, volume 1: The World of Knowbots
(draft) (Washington D.C.: Corporation for National Research
Initiatives; 1988)).

6 Clifford A. Lynch, The Z39.50 Information Retrieval
Protocol: An Overview and Status Report, ACM Sigcomm
Computer Communication Review at 58 (describing Z39.50 as an
OSI application layer protocol that relieves clients from
having to known the structure of data objects to be queried,
and specifies a framework for transmitting and managing
queries and results and syntax for formulating queries).

7 Brewster Kahle, Wide Area Information Server Concepts (Nov. 3, 1989 working copy; updates available from Brewster @THINK. (describing WAIS as "open protocol for connecting user interfaces on workstations and server computers") (describing information servers as including bulletin board services, shared databases, text searching and automatic indexing and computers containing current newspapers and periodicals, movie and television schedules with reviews, bulletin boards and chat lines, library catalogues, Usenet articles).

8 Robert E. Kahn, Deposit, Registration, Recordation in an Electronic Copyright Management System (August 1992) (Corporation for National Research Initiatives, Reston, Virginia).

9 Kahn 1992 at 4.

10 Kahn 1992 at 6.

11 Kahn 1992 at 10.

12 Kahn 1992 at 12.

13 Kahn 1992 at 15.

14 Browsability through techniques like the collapsible outliner function in Microsoft Word for Windows and competing products require more chunking and tagging value in the form of style and text element codes. Handling this additional formatting information through encryption and description processes is problematic.

15 " A 'transfer of copyright ownership' is an assignment, mortgage, exclusive license, or any other conveyance, alienation, or hypothecation of a copyright or of any of the exclusive rights comprised in a copyright, whether or not it is limited in time or place of effect, but not including a non-exclusive license " 17 U.S.C. 101 (1988).

16 17 U.S.C. 204(a) (1988); Valente-Kritzer Video v. Pinckney, 881 F.2d 772, 774 (9th Cir. 1989) (affirming summary judgment for author; oral agreement unenforceable under Copyright Act); Library Publications, Inc. v. Medical Economics Co., 548 F. Supp. 1231, 1233 (E.D. Pa. 1982) (granting summary judgment against trade book publisher who sought enforcement of oral exclusive distribution agreement; transfer of exclusive rights, no matter how narrow, must be in writing), aff'd mem., 714 F.2d 123 (3d Cir. 1983).

17 17 U.S.C. 205 (1988) provides constructive notice of the contents of the recorded document, determining priority as between conflicting transfers, and determines priority as between recorded transfer and non-exclusive license. The former requirement for transfers to be recorded in order for the transferee to maintain an infringement, 17 U.S.C. 205(d), was repealed by the Berne Act Amendments 5.

18 under Adams v. Burke, 84 U.S. (17 Wall.) 453 (1873), a patentee must not attempt to exert control past the first sale. In general, use restrictions may be placed only on licensees, consistent with General Talking Pictures v. Western Elec., 304 U.S. 175 (1938). See generally Baldwin-Lima-Hamilton Corp. v. Tatnall, 169 F. Supp. 1 (E.D.

Pa.1958) (applying no control after purchase rule).

19 See Red-Baron-Franklin Park, Inc. v. Taito Corp., 883 F.2d 275, 278 (4th Cir. 1989) (purchase of video game circuit boards did not create privilege to perform video game under first sale doctrine); United States v. Moore, 604 F.2d 1228, 1232 (9th Cir. 1979) (pirated sound recording not within first sale doctrine in criminal copyright infringement prosecution). But see Mirage Editions, Inc. v. Albuquerque A.R.T. Co., 856 F.2d 1341, 1344 (9th Cir. 1988) (first sale doctrine did not create privilege to prepare derivative work by transferring art in book to ceramic tiles).

20 The way in which the first sale doctrine would impact the electronically imposed use restrictions is by frustrating a breach-of-contract lawsuit by the licensor against a licensee who exceeds the use restrictions. The licensee exceeding the use restrictions would argue that it violates public policy to enforce the restrictions and therefore that state contract law may not impose liability for their violation. See generally Restatement (second) of Contracts 178 (1981) (stating general rule for determining when contract term in unenforceable on grounds of public policy).

21 In addition, as ___ of this paper notes, the Copyright Act itself requires signed writings for transfers of copyright interests. 17 U.S.C. 204(a). (1988).

22 Michael S. Baum & Henry H. Perritt, Jr., Electronic Contracting, Publishing and EDI Law ch. 6 (1991) (contract, evidence and agency issues) [hereinafter "Baum & Perritt"]. Accord, Signature Requirements Under EDGAR, Memorandum from D. Goelzer, Office of the General Counsel, SEC to Kenneth A. Fogash, Deputy Executive Director, SEC (Jan. 13, 1986) (statutory and non-statutory requirements for "signatures" may be satisfied by means other than manual writing on paper in the hand of the signatory . . . "In fact, the electronic transmission of an individual's name may legally serve as that person's signature, providing it is transmitted with the present intention to authenticate.").

23 17 U.S.C. 101 (1988). For copyright purposes, a work is created, and therefore capable of protection, when it is fixed for the first time. 17 U.S.C. 101 (1988). "[I]t makes no difference what the form, manner, or medium of fixation may be - whether it is in words, numbers, notes, sounds, pictures, or any other graphic or symbolic indicia, whether embodied in a physical object in written, printed, photographic, sculptural, punched, magnetic, or any other stable form, and whether it is capable of perception directly or by means of any machine or device 'now known or later developed.'" 1976 U.S. Code Cong. & Admin. News 5659, 5665. The legislative history further says that, "the definition of `fixation' would exclude from the concepts purely of an evanescent or transitory nature -- reproductions such as those projected briefly on a screen shown electronically on a television or other video display or captured momentarily in the `memory' of a computer." 17 U.S.C. 102 note (excerpting from House Report 94-1476).

24 Or, more likely, what is on computer medium read by computer x, such as a magnetic cartridge used for archival records. Further references in the textual discussion to

"what is in computer x now" should be understood to include such computer readable media.

25 Cf. Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 980 (1986) (proof that a printout accurately reflects what is in the computer is too limited a basis for authentication of computer records).

26 In some cases, the electronic transaction will be accomplished by means of a physical transfer of computer readable media. In such a case, this step in the proof would involve proving what was received physically.

27 See generally Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 979 (1986) (citing as examples of authentication Ford Motor Credit Co. v. Swarens, 447 S.W.2d 53 (Ky. 1969) (authentication by establishing relationship between computer-generated monthly summary of account activity and the customer reported on); Ed Guth Realty, Inc. v. Gingold, 34 N.Y.2d 440, 315 N.E.2d 441, 358 N.Y.S.2d 367 (1974) (authentication of summary of taxpayer liability and the taxpayer)).

28 Of course, a paper document signed at the end also is probative of the fact that no alternations have been made. In this sense, a signature requirement telescopes several steps in the inquiry outlined in the text.

29 United States v. Linn, 880 F.2d 209, 216 (9th Cir. 1989) (computer printout showing time of hotel room telephone call admissible in narcotics prosecution). See also United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985) (computer generated toll and billing records in price-fixing prosecution based on testimony by billing supervisor although he had no technical knowledge of system which operated from another office; no need for programmer to testify; sufficient because witness testified that he was familiar with the methods by which the computer system records information).

30 See United States v. Hutson, 821 F.2d 1015, 1020 (5th Cir. 1987) (remanding embezzlement conviction, although computer records were admissible under business records exception, despite trustworthiness challenged based on fact that defendant embezzled by altering computer files; access to files offered in evidence was restricted by special code).

31 Restatement (Second) of Contracts ___ (1981).

32 Cite for when extrinsic evidence is admissible.

33 See Baum & Perritt 2.6; The Electronic Messaging Services Task Force, The Commercial Use of Electronic Data Interchange--A Report and Model Trading Partner Agreement, 45 Bus.Law. 1645 (1990); Jeffrey B. Ritter, Scope of the Uniform Commercial Code: Computer Contracting Cases and Electronic Commercial Practices, 45 Bus.Law. 2533 (1990); Note, Legal Responses to Commercial Transactions Employing Novel Communications Media, 90 Mich.L.Rev. 1145 (1992)

34 Garber v. Harris Trust & Savings Bank, 432 N.E.2d 1309, 1311-1312 (Ill. App. 1982) ("each use of the credit

card constitutes a separate contract between the parties;" citing cases).

It is not quite this simple, because both merchant and credit card customer have separate written contracts with the credit card issuer. But there is no reason that a supplier of information to a Digital Library System and all customers of that system might not have their own contracts with the Digital Library System in the same fashion.

35 Rowland v. Union Hills Country Club, 757 P.2d 105 (Ariz. 1988) (reversing summary judgment for country club officers because of factual question whether club followed bylaws in expelling members); Straub v. American Bowling Congress, 353 N.W.2d 11 (Neb. 1984) (rule of judicial deference to private associations, and compliance with association requirements, counseled affirmance of summary judgment against member of bowling league who complained his achievements were not recognized). But see Wells v. Mobile County Board of Realtors, Inc., 387 So.2d 140 (Ala. 1980) (claim of expulsion of realtor from private association was justiciable and bylaws, rules and regulations requiring arbitration were void as against public policy; reversing declaratory judgment for defendant association).

36 F.R.E. 803(6) (excluding business records from inadmissibility as hearsay); 28 U.S.C. 1732 ("Business Records Act" permitting destruction of paper copies of government information reliably recorded by any means and allowing admission of remaining reliable record).

37 See Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 978-80, 984-85 (1986) (noting body of commentator opinion saying that business records exception and authentication are parallel ways of establishing reliability).

38 See F.R.E. 901(b)(4) (appearance, contents, substance, internal patterns, as examples of allowable authentication techniques).

39 Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 963-64 (1986) (identifying steps and trend resulting in F.R.E.).

40 Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 963 (1986).

41 Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 974 (1986) (reporting four requirements of Manual, and endorsing their use generally).

42 See Henry H. Perritt, Jr., ___, ___ Jurimetrics ___ (1993) (distinguishing between format and content standardization).

43 See Marc Lauritsen, ___ (explaining relationship between substantive legal systems and the field of artificial intelligence).

44 See Thorne, McCarty; Kevin Ashley; and Gardner.

45 It may not be particularly important to limit
competition by consumers, because the consumers will never
have the pointers and the rest of the network
infrastructure.